European Aviation Safety Agency Federal Aviation Administration

Notice of Proposed Amendment 2017-02

Regular update of AMC-20: update of EASA AMC 20-115C and FAA AC 20-115C

RMT.0643

EXECUTIVE SUMMARY

This NPA proposes to amend the EASA AMC 20-115C and the Federal Aviation Administration (FAA) AC 20-115C in order to align these means of compliance, following the selection of non-complex, non-controversial and mature subjects. It is a joint proposal by EASA and the FAA to amend both AMC 20-115C and AC 20-115C.

The objective of the proposed amendments is to update AMC-20 in order to reflect the current state of the art. Overall, this update will significantly increase harmonisation with the FAA, will have no safety, social nor environmental impacts, and will provide for economic benefits by streamlining the certification process.

Action area:	Regular updates/review of rules		
Affected rules:	EASA AMC-20: General acceptable means of compliance for airworthiness of products, parts and appliances; FAA AC 20-115C: Airborne Software Assurance		
Affected stakeholders:	Aircraft and equipment designers and manufacturers		
Driver:	Efficiency/proportionality	**Rulemaking group:**	No
Impact assessment:	Light	**EASA Rulemaking Procedure:**	Standard

Table of contents

1. About this NPA

1.1. How this NPA was developed

EASA, in cooperation with the FAA, developed this NPA in line with Regulation (EC) No 216/2008[1] (hereinafter referred to as the 'Basic Regulation') and the Rulemaking Procedure[2]. This rulemaking activity is included in the EASA 2017–2021 Rulemaking and Safety Promotion Programme[3] under rulemaking task RMT.0643.

It is hereby submitted to all interested parties[4] for consultation.

1.2. How to comment on this NPA

Please submit your comments using the automated **Comment-Response Tool (CRT)** available at **http://hub.easa.europa.eu/crt/**[5].

The deadline for submission of comments is **28 April 2017.**

1.3. The next steps

Following the closing of the public commenting period, EASA and the FAA will review all comments jointly.

Based on the comments received, EASA will develop a decision amending AMC-20 and the FAA will publish a revision to its AC 20-115C.

The comments received, as well as the EASA/FAA responses thereto, will be reflected in a comment-response document (CRD). The CRD will be annexed to the EASA decision. The FAA will publish the same responses to the comments along with the revised AC material on the FAA website.

---

1 Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (OJ L 79, 19.3.2008, p. 1) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1467719701894&uri=CELEX:32008R0216).

2 EASA is bound to follow a structured rulemaking process as required by Article 52(1) of Regulation (EC) No 216/2008. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 18-2015 of 15 December 2015 replacing Decision 01/2012 concerning the procedure to be applied by EASA for the issuing of opinions, certification specifications and guidance material (http://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-18-2015-rulemaking-procedure).

3 http://www.easa.europa.eu/system/files/dfu/RMP-EPAS_2017-2021.pdf

4 In accordance with Article 52 of Regulation (EC) No 216/2008, and Articles 6(3) and 7) of the Rulemaking Procedure. The FAA will publish a notice at https://www.faa.gov/aircraft/draft_docs/ac/.

5 In case of technical problems, please contact the CRT webmaster (crt@easa.europa.eu).

2. In summary — why and what

2.1. Why we need to change the rules — issue/rationale

EASA AMC 20-115C *Software Considerations for Certification of Airborne Systems and Equipment* and the FAA AC 20-115C *Airborne Software Assurance* are similar in the intent, but in some aspects they are not fully aligned. Moreover, they call up identical standards (EUROCAE ED-12C and RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*). Industry associations (AeroSpace and Defence Industries Association of Europe (ASD), General Aviation Manufacturers Association (GAMA), Aerospace Industries Association (AIA)) have requested more harmonisation of the AMC and AC material, particularly on the following topics:

— The conditions under which ED-12B/DO-178B processes can be used for new developments;

— The guidance on tool qualification in the AMC material.

The current situation may create unecessary additional workload and certification delays both for EASA and the FAA, and has a negative impact on applicants.

The current level of safety provided for by this EASA AMC and FAA AC material is considered to be adequate.

2.2. What we want to achieve — objectives

The overall objectives of the EASA system are defined in Article 2 of the Basic Regulation. This proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Section 2.1.

The aim of RMT.0643 is to improve cost-efficiency of the software certification process between EASA and the FAA.

The specific objectives of this proposal are to:

— clarify the conditions under which ED-12B/DO-178B processes can be used for new developments;

— harmonise AMC Section 8 with AC Section 9 regarding the conditions under which a legacy software product can be further developed by reusing an already approved development process;

— allow developers to continue using an existing approved development process even when they introduce new configuration data files (called ‘parameter data items’ in the new ED-12C/ DO-178C standard);

— harmonise the guidance on tool qualification in the AMC material with that of the FAA; and

— compile and streamline the existing acceptable means of compliance and guidance material pertaining to software development assurance (i.e. from EASA Certification Memorandum CM-SWCEH-002 ‘Software Aspects of Certification’ Issue 1 Revision 1, and from FAA Order 8110.49 ‘Software Approval Guidelines’ Change 1) in order to create a single document for software-related guidance.

2.3. How we want to achieve it — overview of the proposals

2.3.1. Definition of the criteria for using ED-12B/DO-178B processes for new developments

AC 20-115C introduced the possibility for applicants to reuse previously approved processes, but without providing criteria under which this is possible. AMC 20-115C did not explicitly introduce this possibility.

To resolve this inconsistency, a new Section 5 has been created in the new AMC and AC material to define precisely the conditions under which ED-12B/DO-178B processes can be used for new developments.

2.3.2. Harmonisation of AMC 20-115C Section 8 with AC 20-115C Section 9

In these documents, the conditions under which a legacy software product could be further developed by reusing an already approved development process were similar in their intent, but were not fully aligned.

Section 9 of AC 20-115C has been taken as the basis for the proposed new text and some portions of the text and of the flow chart (Figure 1) from AC 20-115C have been reworked to provide a fully harmonised set of conditions for the reuse of a legacy process when reusing or modifying an existing software product.

2.3.3. Introducing the possibility of using ED-12C/DO-178C parameter data items (PDI) guidance with ED-12B/DO-178B processes

In both AMC 20-115C and AC 20-115C, the introduction of new configuration data files (called 'parameter data items' in ED-12C/DO-178C) into an existing software program triggered the need to transition to an ED-12C/DO-178C software development process.

Following requests from industry to permit the use of the ED-12C/DO-178C PDI guidance with ED-12B/DO-178B processes, modifications have been introduced in Section 5 and 9 of both the AMC and the AC.

2.3.4. Harmonisation of guidance on tool qualification

Section 10 of AC 20-115C contained specific guidance related to tool qualification. AMC 20-115C did not contain any specific tool qualification guidance.

Section 10 of AC 20-115C has been maintained in AC 20-115D and introduced into AMC 20-115D.

2.3.5. Compilation and streamlining of material pertaining to software development assurance

The available EASA and FAA software development assurance material (other than AMC 20-115C and AC 20-115C) has been reviewed and analysed in order to identify material that should be embedded in the updated AMC/AC material.

The following guidance has been streamlined and included in Section 8 of both AMC 20-115D and AC 20-115D:

— Guidance for field loadable software (FLS). Rationale: Section 2 of EUROCAE ED-12C and RTCA DO-178C is admitedly not considered as guidance as it pertains to system-level objectives and activities; there are, however, implicit objectives applicable to a software developer that need to be identified in the updated AMC/AC material. Existing material from EASA CM-SWCEH-002 Issue 1 Revision 1 and from FAA Order 8110.49 Change 1 has been streamlined down to minimal guidance for software developers only.

— Guidance for user modifiable software (UMS). Rationale: Section 2 of EUROCAE ED-12C and RTCA DO-178C is admitedly not considered as guidance as it pertains to system-level objectives and activities; there are, however, implicit objectives applicable to a software developer that need to be identified in the updated AMC/AC material. Existing material from EASA CM-SWCEH-002 Issue 1 Revision 1 and from FAA Order 8110.49 Change 1 has been streamlined down to minimal guidance for software developers only.

Moreover, two additional guidance material documents have been created (GM to AMC 20-115D on the EASA side, and AC 00-SW on the FAA side) in order to keep and streamline 'best practices' topics that were considered to be important clarifications:

— Clarification on software change impact analyses (CIAs). Rationale: The expectations in terms of scope and content of a CIA are not clarified anywhere in the existing software development assurance material. Existing material from FAA Order 8110.49 Change 1 has been reused and streamlined.

— Clarification on data coupling and control coupling. Rationale: Objective A-7 (8) of ED-12C/ DO-178C and ED-12B/DO-178B leads to typical pitfalls that can be helpful to clarify from the beginning of a software development. Existing material from EASA CM-SWCEH-002 Issue 1 Revision 1 has been streamlined down to a minimal set of clarifications.

— Clarification on error handling at design level. Rationale: Section 6.3.4.f. of ED-12C/DO-178C and ED-12B/DO-178B identifies potential sources of errors that require specific activities focused at source code review level; however, in order to protect against foreseeable unintended software behaviour, it is beneficial to handle these sources of error at design level. Existing material from EASA CM-SWCEH-002 Issue 1 Revision 1 has been reworked to clarify the expectations regarding this ED-12C/DO-178C and ED-12B/DO-178B activity.

2.4. What are the expected benefits of the proposals

Overall, the proposed amendments would significantly increase the harmonisation of the EASA software guidance with that of the FAA, would have no safety, social nor environmental impacts, and would provide for economic benefits by streamlining the certification process.

No drawbacks are expected.

3. Proposed amendments and rationale in detail

As the goal of this activity is to harmonise the text of the EASA AMC with that of the FAA AC, the amendments to the EASA AMC 20-115C and the FAA AC 20-115C are significant. Therefore, a completely new text is proposed, without any detailed tracking of change information.

The draft EASA decision consists of:

— a draft acceptable means of compliance (AMC 20-115D): see Section 3.1; and

— a draft guidance material document (GM to AMC 20-115D): see Section 3.2.

The draft FAA guidance consists of:

— a draft acceptable means of compliance (AC 20-115D): see Section 3.1; and

— a draft best practices document (AC 00-SW): see Section 3.2.

Note: To facilitate the identification of the differences between the EASA and the FAA text proposals, both the AMC and AC material has been compiled into one single paragraph numbered 3.1 of this NPA. Similarly, the GM and AC 00-SW have been compiled into one single paragraph (numbered 3.2 of this NPA). Markings using square brackets '**[**…**]**' and '**<AMC>**'/'**<AC>**' markers have been introduced to facilitate the identification of those differences.

3.1. Draft acceptable means of compliance (EASA AMC / FAA AC)

[<AMC> AMC 20-115D: Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( ) for Product Certification or ETSO Authorisation**]**
[<AC> AC 20-115D: Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )**]**

1. Purpose [of this Advisory Circular (AC)]

a. This **[**AMC**]/[**AC**]** describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the software aspects of airborne systems and equipment certification. **[<AMC>** Compliance with this AMC is not mandatory and, therefore, an applicant may elect to use an alternative means of compliance. However, the alternative means of compliance must meet the relevant requirements, ensure an equivalent level of software safety, and be approved by EASA on a product or ETSO article basis.**] [<AC>** This AC is not mandatory and does not constitute a regulation. However, if you use the means described in the AC, you must follow it in all important respects.**]**

b. This **[**AMC recognises**]/[**AC recognizes**]** the following EUROCAE and RTCA documents:

(1) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012 and RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.

(2) EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012 and RTCA DO-330, *Software Tool Qualification Considerations*, dated December 13, 2011.

(3) EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012 and RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(4) EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012 and RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(5) EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012, and RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.

Note: EUROCAE ED is hereafter referred to as ED; RTCA DO is hereafter referred to as DO. Where the notation ED-XXX/DO-XXX appears in this document, refer to the applicable document pertaining to your processes.

c. This **[**AMC**]/[**AC**]** identifies the following as supporting documents: ED-94C, *Supporting Information for ED-12C and ED-109A*, and DO-248C, *Supporting Information for DO-178C and DO-278A*. ED-94C**/**DO-248C contains a collection of frequently asked questions (FAQs) and discussion papers (DPs) compiled and approved by the authors of ED-12C and DO-178C to provide clarification on the guidance contained in ED-12C/DO-178C.

d. References to use of ED-12C/DO-178C in this **[**AMC**]/[**AC**]** include use of ED-215/DO-330 and supplements ED-218/DO-331, ED-217/DO-332 and ED-216/DO-333, as applicable.

e. This **[**AMC**]/[**AC**]** establishes guidance for using existing ED-12B/DO-178B processes for new development.

f. This **[**AMC**]/[**AC**]** also establishes guidance for transitioning to ED-12C/DO-178C when making modifications to software previously approved using ED-12/DO-178, ED-12A/DO-178A, or ED-12B/ DO-178B.

g. This **[**AMC**]/[**AC**]** also explains the use of ED-12C/DO-178C for **[**European Technical Standard Order (ETSO) authorisations**]/[**Technical Standard Order (TSO) authorizations**]**.

h. [<AMC> <Reserved>**]**

h. [<AC> This AC does not obligate the FAA to approve any data or perform any activities as specified within the referenced RTCA and EUROCAE documents.**]**

2. Applicability. We wrote this **[**AMC**]/[**AC**]** for applicants, design approval holders, and developers of airborne systems and equipment containing software to be installed on **[**type-certified**]/[**type certificated**]** aircraft, engines, and propellers.

3. Cancellation. This **[**AMC**]/[**AC**]** cancels **[**AMC 20-115C, *Software Considerations in Airborne Systems and Equipment Certification*, dated 12 September 2013**]/[**AC 20-115C, *Airborne Software Assurance*, dated July 19, 2013**]**.

4. Background

a. ED-12C/DO-178C, Appendix A, Section 3, provides a summary of differences between ED-12C/DO-178C and ED-12B/DO-178B. The EUROCAE and RTCA documents identified in subparagraph 1.b. of this **[**AMC**]/[**AC**]** provide guidance for establishing software life cycle planning, development, verification, configuration management, quality assurance, and certification liaison processes to be used in the development of software for airborne systems. The guidance provided in these documents is in the form of:

(1) Objectives for software life cycle processes;

(2) Activities that provide a means for satisfying the objectives; and

(3) Descriptions of the evidence that indicate that the objectives have been satisfied.

b. The technical content of this **[**AMC**]/[**AC**]** is as far as practicable **[**harmonised with Federal Aviation Administration (FAA) AC 20-115D**]/[**harmonized with European Aviation Safety Agency (EASA) AMC 20-115D**]**, equally based on ED-12C/DO-178C.

5. Using ED-12B/DO-178B Processes and Procedures for New Development.

a. Applicants who have established software development assurance processes using ED-12B/DO-178B may continue to use those processes for new software development and certification projects, provided the following criteria are met:

(1) The software development assurance processes can be shown to have no known process deficiencies, such as those discovered during internal or external audit or review, or identified in open problem report(s) resulting in non-compliance to one or more ED-12B/DO-178B objectives. Additionally, evidence that the process has produced software with **[**favourable**]/[**favorable**]** usage history, based on evaluation of previous projects, including review of safety-related service difficulties, airworthiness directives, and process-related problem reports may be requested.

(2) The processes have been previously used to develop software that has been used in a certified product at a software level at least as high as the software level of the software to be developed.

(3) Model-based development, object-oriented technology, or formal methods will not be used, unless processes incorporating these methods were evaluated and found to be acceptable by **[**EASA**]/[**the FAA**]**. These processes should have been developed in accordance with **[**EASA**]/[**FAA**]** guidance specific to the technique, such as that contained in associated **[**Certification Review Item (CRI) or published Certification Memorandum (CM)**]/[**issue paper or published advisory circular**]**.

(4) Existing processes for using configuration data (as defined under “Parameter Data Item” in ED-12C/DO-178C) were evaluated and found to be acceptable by **[**EASA**]/[**the FAA**]**. In the absence of processes for using configuration data, the applicant should establish new processes for using parameter data items in accordance with ED-12C/DO-178C.

(5) There are no significant changes to the software processes described in the plans or to the software development environment. This should be supported through analysis of changes to the previously accepted software development processes and environment.

(6) You do not intend to declare the proposed software as having satisfied ED-12C/DO-178C.

b. If the criteria of subparagraph 5.a. are not met, you should upgrade your processes and develop the new software using ED-12C/DO-178C; tool qualification processes should be addressed in accordance with ED-12C/DO-178C section 12.2 of ED-12C/DO-178C and paragraph 10.c of this document.

c. Applicants or developers who are establishing new software life-cycle processes should do so in accordance with ED-12C/DO-178C.

6. Using EUROCAE ED-12C and RTCA DO-178C [<AC> for Type Certification]. ED-12C/DO-178C is an acceptable means of compliance for the software aspects of **[**product**]/[**type**]** certification **[<AMC>** or ETSO authorisation**]**. When you use ED-12C/DO-178C:

a. [The applicant**]/[**You**]** should satisfy all the objectives associated with the software level assigned to the software components and develop all the associated life-cycle data as specified in the outputs listed in the ED-12C/DO-178C Annex A tables and, where applicable, the ED-215/DO-330, ED-216/DO-333, ED-217/DO-332, and ED-218/DO-331 Annex A tables. **[**The applicant**]/[**You**]** should plan and execute activities that will satisfy each objective. **[<AC>** If the FAA chooses not to be involved in the certification liaison process, you can consider the certification liaison process objectives and activities to be satisfied after you have produced the life-cycle data specified in Table(s) A-10 of ED-12C/DO-178C, ED-215/DO-330 and supplements, as applicable.**]**

b. [The applicant**]/[**You**]** should submit **[**to EASA, **]/[**, **]** as a minimum, the life-cycle data specified in section 9.3 of ED-12C/DO-178C and section 9.0.a of ED-215/DO-330, as applicable for tool qualification **[<AC>**, to the appropriate project certification office**]**. **[**EASA's**]/[**Our**]** involvement in **[**the**]/[**your**]** software development assurance processes will be at **[**its**]/[**our**]** discretion. Regardless of **[**EASA**]/[**our**]** involvement, it is **[**the applicant's**]/[**your**]** responsibility to perform the planned activities and produce the life-cycle data necessary to satisfy all applicable objectives.

c. Section 9.4 of ED-12C/DO-178C specifies the software life cycle data related to the type design of the certified product. However, not all of the specified data applies to all software levels. If a data item specified in section 9.4 of ED-12C/DO-178C is not required in Table A-2 or Table A-10 for a given software level, then this data item is not part of the type design data.

d. You should make available to **[**EASA**]/[**us**],** upon request, any of the data described in section 11 of ED-12C/DO-178C, applicable tool qualification data, data outputs from any applicable supplements, and any other data needed to substantiate satisfaction of all the applicable objectives.

e. [EASA**]/[**The FAA**]** may publish acceptable means of compliance for specific **[**Certification Specifications**]/[**regulations**]**, stating the required relationship between the criticality of the software-based systems and the software levels as defined in ED-12C/DO-178C. Such acceptable means of compliance will take precedence over the application of section 2.3 of ED-12C/DO-178C.

7. [<AMC> Reserved]

7. [<AC> Using DO-178C for TSO Authorisation

a. Requirements for submitting software documentation for TSO authorisation are stated in each applicable TSO.

b. Many FAA TSOs do not specify DO-178C for software development assurance. Although we recommend using DO-178C, paragraph 5 or paragraph 9 of this AC may be used to determine whether your use of an earlier version is acceptable. If you use a version other than that specified in the TSO, you should request a deviation in accordance with the requirements of Title 14 of the Code of Federal Regulations (14 CFR) part 21, Subpart O.**]**

8. Guidance applicable to ED-12B/DO-178B or ED-12C/DO-178C.

a. Use of Supplements with ED-12C/DO-178C. ED-218/DO-331, ED-217/DO-332 and ED-216/DO-333 are supplements that address certain software development techniques. Supplements add, delete or modify objectives, activities and life-cycle data in ED-12C/DO-178C. You should apply the guidance within a particular supplement when you use the addressed technique. If you intend to use multiple software development techniques together, more than one ED-12C/DO-178C supplement applies. You cannot use supplements as stand-alone documents.

(1) When using one or more supplements, your Plan for Software Aspects of Certification (PSAC) should describe:

(a) How you will apply ED-12C/DO-178C and the supplement(s) together.

(b) How you will address the applicable ED-12C/DO-178C objectives and those added or modified by the supplement(s), which objectives from which documents apply to which software components, and how your planned activities will satisfy all applicable objectives.

(2) If you intend to use any techniques addressed by the supplements to develop a qualified tool, then you should use the applicable supplements for those objectives (tool qualification levels (TQLs) 1, 2, 3 and 4 only). Your Tool Qualification Plan should describe:

(a) How you will apply ED-215/DO-330 and the supplement guidance to the tool development or verification.

(b) How you will address the applicable ED-215/DO-330 objectives and those added or modified by the supplements, which objectives apply to which components of each software tool, and how the planned activities will satisfy all the applicable objectives.

(3) The intent of this subparagraph is to provide clarification and completeness of section MB.6.8.1 of ED-218/DO-331. If you are using models as defined in section MB.1.0 of ED-218/DO-331 as the basis for developing software, you should apply the guidance in ED-218/DO-331. When applying section MB.6.8.1 of ED-218/DO-331, you should:

(a) Identify what reviews and analyses objectives are planned to be satisfied by simulation alone or in combination with reviews and analyses; all other objectives should be satisfied by reviews and analyses as described in section MB.6.3 of ED-218/DO-331.

(b) For each identified objective justify in detail how the simulation activity alone or in combination with reviews and analyses fully satisfies the specific reviews and analyses objective.

b. Guidance for Field Loadable Software (FLS). This section supplements ED-12C/DO-178C and ED-12B/DO-178B. Use this guidance in addition to ED-12C/DO-178C and ED-12B/DO-178B when using FLS in your project.

(1) As the developer, you should provide the necessary information to support the system-level guidance identified in section 2.5.5 of ED-12C/DO-178C, items a, b, c and d, and section 2.5 of ED-12B/DO-178B, items a, b, c and d.

(2) The FLS should be protected against corruption or partial load to an integrity level appropriate for the software level of the FLS.

(3) The FLS part number, when loaded in the airborne equipment, should be verifiable by appropriate means.

(4) Protection mechanisms should be implemented to prevent inadvertent enabling of the field loading function during flight or any other safety-critical phase.

c. Guidance for User Modifiable Software (UMS). This section supplements ED-12C/DO-178C and ED-12B/DO-178B. You should use this guidance in addition to ED-12C/DO-178C and ED-12B/DO-178B when using UMS in your project.

(1) As the developer, you should provide the necessary information to support system-level guidance identified in section 2.5.2 of ED-12C/DO-178C, items a, b, c and f, and section 2.4 of ED-12B/DO-178B, items a and b.

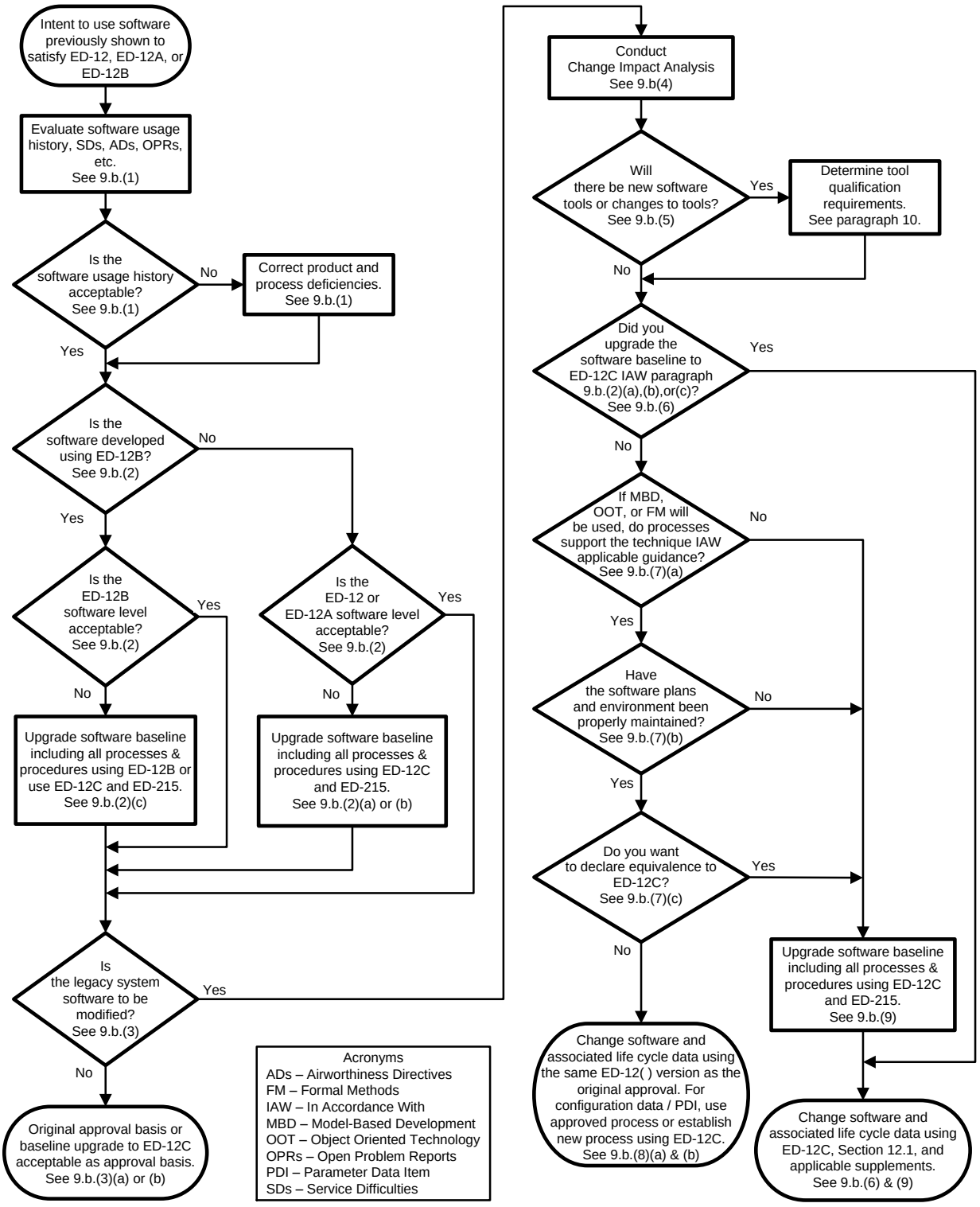
(2) The modifiable part of the component should be developed to a software level at least as high as the software level assigned to that software component.

9. Modifying and Reusing Software Approved using ED-12/DO-178, ED-12A/DO-178A or ED-12B/DO-178B

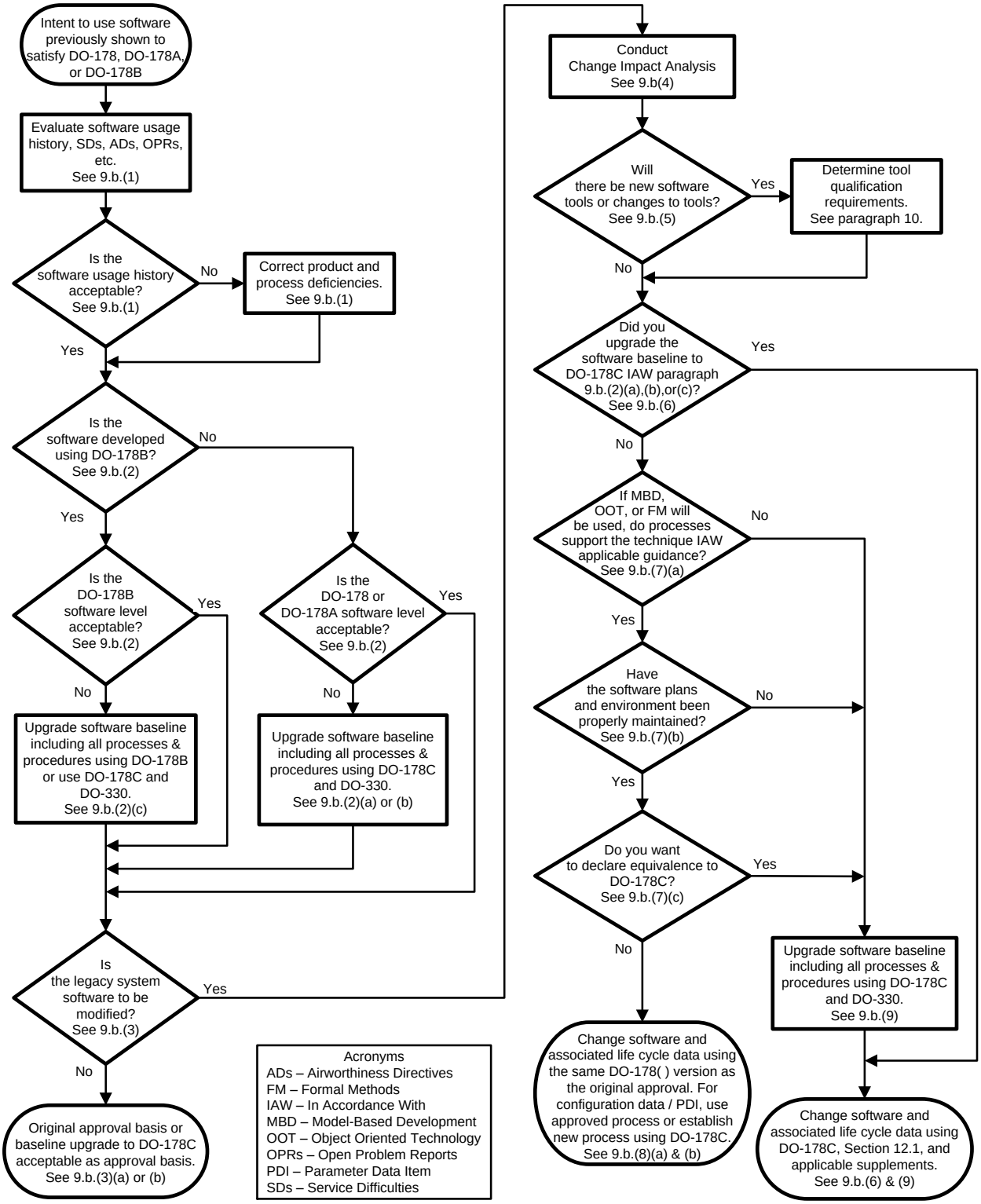
a. We previously approved the software for many airborne systems using ED-12/DO-178, ED-12A/DO-178A or ED-12B/DO-178B as a means of compliance. In this **[**AMC**]**/**[**AC**]**, we refer to these systems as legacy systems, and to the software as legacy system software. In this paragraph, we describe how to demonstrate compliance with the software aspects of certification for an application that includes modifications to legacy system software or use of unmodified legacy system software.

b. Figure 1 presents a flow chart for using legacy system software. Use the flow chart while following the procedures in this subparagraph if you are modifying or reusing legacy system software. Although these procedures will apply to the majority of projects, you should coordinate situations that do not follow this flow with **[**EASA**]**/**[**the certification office**]**.

[<AMC> Figure 1 — Legacy System Software Process Flow Chart]



[<AC> Figure 1 — Legacy System Software Process Flow Chart]



(1) Assess the legacy system software to be modified or reused for its usage history from previous installations. If the software has safety-related service difficulties, airworthiness directives, or open problem reports that may have a safety impact on the proposed installation, correct the known software and development process deficiencies prior to modifying or reusing the software.

(2) The system safety process assigns the minimum development assurance level based on the severity classifications of failure conditions for a given function. The ED-12B/DO-178B software levels are consistent with the ED-12C/DO-178C software levels. However, ED-12/DO-178 and ED-12A/DO-178A were published prior to establishment of the software levels addressed in ED-12B/DO-178B and ED-12C/DO-178C. Use Table 1 to determine if your legacy system software level satisfies the software level assigned by the system safety process for the proposed installation. A "✓" in the intersection of the row and column indicates that the legacy system software level is acceptable. For example, legacy system software with development assurance to ED-12A/DO-178A software Level 2 can be considered to satisfy software Levels B, C, and D. A blank indicates that the software level is not acceptable. Therefore, the ED-12A/DO-178A software developed to software Level 2 would not be acceptable where software Level A is required.

Table 1 — Software Development Assurance Level Relationships

Assigned Software Level	**Legacy System Software Level per ED-12B/ DO-178B**				**Legacy System Software Level per ED-12A/ DO-178A**			**Legacy System Software Level per ED-12/DO-178**		
	A	***B***	***C***	***D***	***1***	***2***	***3***	***Critical***	***Essential***	***Non-essential***
A	✓				✓			✓		
B	✓	✓			✓	✓		✓		
C	✓	✓	✓		✓	✓		✓	✓	
D	✓	✓	✓	✓	✓	✓		✓	✓	

(a) If your legacy system software was developed to software Level Essential using ED-12/DO-178 and was previously accepted by the certification authority as acceptable for software Level B, it remains acceptable for the new project. If the ED-12/DO-178 legacy system software was not previously assessed, or the software level is not acceptable, then upgrade the software development baseline, including all processes and procedures (including tool qualification processes), using section 12.1.4 of ED-12C/DO-178C, and ED-215/DO-330.

(b) If your legacy system software was developed using ED-12A/DO-178A, and the software level is not acceptable, upgrade the software development baseline, including all processes and procedures (including tool qualification processes), using section 12.1.4 of ED-12C/DO-178C, and ED-215/DO-330.

(c) If your legacy system software was developed using ED-12B/DO-178B, and the software level is not acceptable, upgrade the software development baseline, including all processes and procedures (including tool qualification processes), using section 12.1.4 of ED-12B/DO-178B or ED-12C/DO-178C, and ED-215/DO-330.

(3) If the usage history of your legacy system software is acceptable, the software level has a "✓" entry in Table 1 (or the baseline has been upgraded appropriately), and modifications to the software are not required, then:

(a) The original approval may serve as the basis for the software in the installation approval of the proposed system.

(b) If you upgraded the software development baseline using ED-12C/DO-178C and updated all processes and procedures, including tool qualification processes, to ED-12C/DO-178C and ED-215/DO-330, then you may declare your software as equivalent to satisfying ED-12C/DO-178C. However, you cannot declare your unmodified tools as equivalent to having satisfied ED-12C/DO-178C and ED-215/DO-330. All subsequent modifications to all your software and tools are to be made using your processes and procedures that satisfy ED-12C/DO-178C and ED-215/DO-330.

(4) If modifications to the software are required, conduct a software change impact analysis (CIA) to determine the potential impact of the modifications on the continued operational safety of the aircraft on which the system and software components are to be installed. The CIA should determine the extent of the modifications, the impact of those modifications, and what verification is required to ensure that the modified software performs its intended function and continues to satisfy the identified means of compliance.

(a) Identify the software changes to be incorporated and conduct a CIA consisting of one or more analyses associated with the software change as identified in section 12.1 of ED-12C/DO-178C.

(b) Conduct the verification as indicated by the CIA.

(c) Summarise the results of the CIA in the Software Accomplishment Summary (SAS).

(5) If new software tools or modifications to tools are needed, refer to paragraph 10 of this **[**AMC**]/[**AC**]** to determine tool qualification requirements.

(6) If you upgraded the software baseline to ED-12C/DO-178C in accordance with subparagraph 9.b.(2), make all modifications to the software using section 12.1 of ED-12C/DO-178C. If you want to declare your software as equivalent to satisfying ED-12C/DO-178C, your equivalence declaration applies to both modified and unmodified software and is valid even if you use unmodified tools that have not been qualified using ED-12C/DO-178C. However, you cannot declare your unmodified tools as equivalent to having satisfied ED-12C/DO-178C and ED-215/DO-330. All subsequent modifications to all your software and tools are to be made using your processes and procedures that satisfy ED-12C/DO-178C and ED-215/DO-330.

(7) If you want to use your existing processes to make modifications to your legacy system software using the version of ED-12( )/DO-178( ) (i.e. ED-12/DO-178, ED-12A/DO-178A or ED-12B/DO-178B) that was used for the original software approval, you may do so provided all the following conditions are met:

(a) Model-based development, object-oriented technology or formal methods will not be used unless processes incorporating these methods were evaluated and found to be acceptable by **[**EASA**]/[**the FAA**]**. These processes should have been developed in accordance with the **[**EASA**]/[**FAA**]** guidance specific to the technique, such as that contained in associated **[**Certification Review Item (CRI) or published Certification Memorandum (CM)**]/[**issue paper or published advisory circular**]**.

(b) You have maintained, and can still use, the software plans, processes, and life-cycle environment, including process improvements and changes resulting from subparagraph 9.b.(2)(c).

(c) You do not intend to declare the proposed software as having satisfied ED-12C/DO-178C.

(8) If the conditions in subparagraph 9.b.(7) are satisfied:

(a) You may accomplish all modifications to the software using the same ED-12( )/ DO-178( ) version as the original approval. However, you may not declare your software as equivalent to satisfying ED-12C/DO-178C.

(b) You may use existing processes for configuration data (as defined under 'Parameter Data Item' in ED-12C/DO-178C) that were evaluated and found to be acceptable by **[**EASA**]/[**the FAA**]**. In the absence of processes for using configuration data, **[**the applicant**]/[**you**]** should establish new processes for using parameter data items in accordance with ED-12C/DO-178C.

(9) If any of the conditions in subparagraph 9.b.(7) are not satisfied, update all your processes and procedures (including tool qualification processes), using ED-12C/DO-178C and ED-215/DO-330, and make all modifications to the software using section 12.1 of ED-12C/DO-178C. If you want to declare your software as equivalent to satisfying ED-12C/DO-178C, your declaration applies to both the modified and unmodified software and is valid even if you use unmodified tools that have not been qualified using ED-12C/DO-178C and ED-215/DO-330. However, you cannot declare your unmodified tools as equivalent to having satisfied ED-12C/DO-178C and ED-215/DO-330. All subsequent modifications to all your software and tools are to be made using your processes and procedures that satisfy ED-12C/DO-178C and ED-215/DO-330.

10. Tool Qualification. Section 12.2 of ED-12C/DO-178C, and ED-215/DO-330 provide an acceptable method for tool qualification. ED-215/DO-330 contains its own complete set of objectives, activities, and life cycle data for tool qualification.

a. If your legacy system software was previously approved using ED-12/DO-178 or ED-12A/DO-178A, and you intend to use a new or modified tool for modifications to the legacy system software, use the criteria of section 12.2 of ED-12C/DO-178C to determine if tool qualification is needed. If you need to qualify the tool, use the software level assigned by the system safety assessment for determining the required Tool Qualification Level (TQL), and use ED-215/DO-330 for the applicable objectives, activities, and life cycle data. You may declare your qualified tool as having satisfied ED-215/DO-330 but not the legacy system software as equivalent to having satisfied ED-12C/DO-178C.

b. If your legacy system software was previously approved using ED-12B/DO-178B, and you do not intend to declare equivalence to satisfying ED-12C/DO-178C, you can either:

(1) Use your ED-12B/DO-178B tool qualification processes for qualifying new or modified tools in support of modifications to ED-12B/DO-178B legacy system software, or

(2) Update your tool qualification processes and qualify the tool using ED 215/DO-330; use Table 2 of this document for determining the required TQL. You may then declare your qualified tool as having satisfied ED-215/DO-330

c. If your legacy system software was previously approved using ED-12B/DO-178B, you intend to declare equivalence to satisfying ED-12C/DO-178C, and you have ED-12B/DO-178B legacy tools that need to be qualified, follow the guidance of this subparagraph.

(1) ED-12C/DO-178C establishes five levels of tool qualification based on the tool use and its potential impact on the software life cycle processes (see section 12.2.2 and Table 12-1 of ED-12C/DO-178C). However, ED-12C/DO-178C does not address the use of tools previously qualified to the ED-12B/DO-178B criteria. For a tool previously qualified as an ED-12B/DO-178B development tool or verification tool, use Table 2 (below) to determine the correlation between the ED-12B/DO-178B tool qualification type and ED-12C/DO-178C tool criteria and tool qualification levels (TQLs).

Table 2 — Correlation Between ED-12B/DO-178B Tool Qualification Type and ED-12C/DO-178C Tool Criteria and TQL

ED-12B/ DO-178B Tool Qualification Type	*Software Level*	*ED-12C/ DO-178C Tool Criteria*	*[ED-12C/ED-215]/ [DO-178C/DO-330] TQL*
Development	A	1	TQL-1
Development	B	1	TQL-2
Development	C	1	TQL-3
Development	D	1	TQL-4
Verification	A, B	2	TQL-4
Verification	C, D	2	TQL-5
Verification	All	3	TQL-5

(2) Development Tools Previously Qualified Using ED-12B/DO-178B.

(a) If the ED-12B/DO-178B software level assigned to the tool correlates with or exceeds the required TQL established by ED-12C/DO-178C, you may continue to use your ED-12B/DO-178B tool qualification processes. If there are changes to the tool's operational environment or to the tool itself, then you should conduct a tool change impact analysis according to section 11.2.2 or 11.2.3 of ED-215/DO-330, respectively, and perform changes using your ED-12B/DO-178B tool qualification processes.

(b) If the ED-12B/DO-178B software level assigned to the tool does not satisfy the required TQL, you should requalify the tool using ED-215/DO-330.

(c) You may declare your tool as equivalent to having satisfied ED-215/DO-330 if all changes to the tool and your tool qualification processes satisfy ED-215/DO-330.

(3) Verification Tools Previously Qualified Using ED-12B/DO-178B.

(a) If TQL-5 is the required tool qualification level, and your verification tool was previously qualified using ED-12B/DO-178B:

(i) You may continue to use your ED-12B/DO-178B tool qualification process.

(ii) If there are changes to the tool or the tool's operational environment, you should conduct a tool change impact analysis and reverify the tool using your ED-12B/DO-178B tool qualification processes or requalify the tool using ED-215/DO-330.

(b) If TQL-4 is the required tool qualification level, you should requalify your verification tool using ED-215/DO-330.

(c) You may declare your tool as equivalent to having satisfied ED-215/DO-330 if all changes to the tool and your tool qualification processes satisfy ED-215/DO-330.

11. [<AMC> Related Regulatory, Advisory, and Industry Material.

a. Related EASA Certification Specifications (CSs).

(1) CS-23, *Certification Specifications and Acceptable Means of Compliance for Normal, Utility, Aerobatic, and Commuter Category Aeroplanes,* Amendment 4, dated 15 July 2015.

(2) CS-25, *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes*, Amendment 18, dated 22 June 2016.

(3) CS-27, *Certification Specifications and Acceptable Means of Compliance for Small Rotorcraft,* Amendment 4, dated 30 November 2016.

(4) CS-29, *Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft,* Amendment 4, dated 30 November 2016.

(5) CS-E, *Certification Specifications and Acceptable Means of Compliance for Engines,* Amendment 4, dated 12 March 2015, and AMC 20-3A, *Certification of Engines Equipped with Electronic Engine Control Systems,* dated 12 September 2013.

(6) CS-P, *Certification Specifications for Propellers,* Amendment 1, dated 16 November 2006, and AMC 20-1, *Certification of Aircraft Propulsion Systems Equipped with Electronic Control Systems,* dated 26 December 2007.

(7) CS-ETSO, *Certification Specifications for European Technical Standard Orders,* Amendment 12, dated 15 December 2016.

(8) CS-APU, *Certification Specifications for Auxiliary Power Units,* dated 17 October 2003, and AMC 20-2A, *Certification of Essential APU Equipped with Electronic Controls,* dated 12 September 2013.

b. FAA Advisory Circulars (ACs)

(1) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes*.

(2) AC 27-1309, *Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*).

(3) AC 29-1309, *Equipment, Systems, and Installations* (included in AC 29-2, *Certification of Transport Category Rotorcraft*).

c. Industry Documents

(1) EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print).

(2) EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print).

(3) EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992.

(4) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012.

(5) EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012.

(6) EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012.

(7) EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012.

(8) EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012.

(9) EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012.

(10) RTCA DO-178, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 1982 (no longer in print).

(11) RTCA DO-178A, *Software Considerations in Airborne Systems and Equipment Certification*, dated March 1985 (no longer in print).

(12) RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, dated 1 December 1992.

(13) RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated 13 December 2011.

(14) RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*, dated 13 December 2011.

(15) RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, dated 8 November 2005.

(16) RTCA DO-330, *Software Tool Qualification Considerations*, dated 13 December 2011.

(17) RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A,* dated 13 December 2011.

(18) RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated 13 December 2011.

(19) RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated 13 December 2011.**]**

11. [<AC> Related Regulatory, Advisory, and Industry Material

a. 14 CFR Applicable Sections. 14 CFR parts 21, 23, 25, 27, 29, 33 and 35.

b. FAA Advisory Circulars (ACs).

(1) AC 20-170, *Integrated Modular Avionics Development, Verification, Integration and Approval using RTCA DO-297 and Technical Standard Order C-153*.

(2) AC 20-171, *Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment*.

(3) AC 20-174, *Development of Civil Aircraft and Systems.*

(4) AC 21-50, *Installation of TSOA Articles and LODA Appliances.*

(5) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes.*

(6) AC 25.1309-1, *System Design and Analysis.*

(7) AC 27-1309*, Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*)*.*

(8) AC 29-1309, *Equipment, Systems, and Installations* (included in AC 29-2, *Certification of Transport Category Rotorcraft*)*.*

(9) AC 33.28-1, *Compliance Criteria for 14 CFR § 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems.*

(10) AC 33.28-2, *Guidance Material for 14 CFR 33.28, Reciprocating Engines, Electrical and Electronic Engine Control Systems*.

(11) AC 33.28-3, *Guidance Material for 14 CFR § 33.28, Engine Control Systems.*

(12) AC 35.23-1, *Guidance Material for 14 CFR 35.23, Propeller Control Systems*.

c. Industry Documents

(1) RTCA DO-178, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 1982 (no longer in print).

(2) RTCA DO-178A, *Software Considerations in Airborne Systems and Equipment Certification*, dated March 1985 (no longer in print).

(3) RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1, 1992

(4) RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.

(5) RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*, dated December 13, 2011.

(6) RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, dated November 8, 2005.

(7) RTCA DO-330, *Software Tool Qualification Considerations*, dated 13 December 2011.

(8) RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A,* dated December 13, 2011.

(9) RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(10) RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(11) EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print).

(12) EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print).

(13) EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992.

(14) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012.

(15) EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012.

(16) EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012.

(17) EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012.

(18) EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012.

(19) EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012.**]**

12. [<AMC> Availability of Documents

— EASA Certification Specifications (CSs) and Acceptable Means of Compliance (AMC) may be downloaded from the EASA website: www.easa.europa.eu.

— FAA Advisory Circulars (ACs) may be downloaded from the FAA website: www.faa.gov.

— EUROCAE documents may be purchased from:

European Organisation for Civil Aviation Equipment
102 rue Etienne Dolet, 92240 Malakoff, France
Telephone: +33 1 40 92 79 30, Fax: +33 1 46 55 62 65
(E-mail: eurocae@eurocae.net, website: www.eurocae.net)

— RTCA documents may be purchased from:

RTCA, Inc.
1150 18th Street NW, Suite 910, Washington DC 20036, USA
(E-mail: info@rtca.org, website: www.rtca.org).**]**

12. [<AC> Where to Find this AC.

a. You may find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/.

b. If you have suggestions for improvement or changes, you may use the template at the end of this AC.

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to 9-AWA-AVS-AIR500-Coord@faa.gov, or (2) faxing it to the attention of the AIR Directives Management Officer at 202-267-3983.

Subject: _____ Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

☐ In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____

3.2. Draft EASA guidance material (GM) / FAA AC 00-SW.

[<AC> AC 00-SW: Best Practices for Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )

1.0 Purpose. This advisory circular (AC) provides information in the form of "best practices" and, as such, is not intended as guidance but rather as complementary information to ED-12C/DO-178C (and related documents) and AC 20-115D.

2.0 Audience. We wrote this AC as a means of assisting applicants, design approval holders and developers of airborne systems and equipment containing software intended to be installed on type certificated aircraft, engines, and propellers.

3.0 Best practices.]

[<AMC> GM1 to AMC 20-115D]/[<AC> 3.1] Software Change Impact Analyses (CIA).

a. These practices provide complementary information to ED-12C/DO-178C and ED-12B/DO-178B, Sections 12.1.1, 12.1.2 and 12.1.3, and **[**AMC 20-115D**]/[**AC 20-115D**]**, subparagraph 9.b.(4). You may **[<AMC>** use this guidance material**]/[<AC>** consider using these best practices**]** when you need to conduct a software CIA.

b. A CIA identifies the released software baseline upon which the proposed software is to be built, providing:

(1) A summary of the changes and impact of the changes;

(2) A listing and descriptions of the open problem reports and/or change requests related to those changes; and

(3) A listing of new functions to be activated and/or implemented.

c. The CIA addresses changes to the following items, where applicable:

(1) Software level;

(2) Development or verification environment;

(3) Software processes;

(4) Tools (e.g. when a new tool version is introduced or a tool's use is modified);

(5) Processor or other hardware components and interfaces;

(6) Configuration data, especially when activating or deactivating functions;

(7) Software interface characteristics and input/output requirements; and/or

(8) Software requirements, design, architecture, and code components, where such changes are not limited to the modified life-cycle data, but should also consider the ones affected by the change.

d. For each applicable item in subparagraph c. above, a CIA describes the resulting impact and identifies the activities to be performed to satisfy ED-12C/DO-178C and ED-12B/DO-178B and to continue to satisfy requirements for safe operation.

[<AMC> GM2 to AMC 20-115D]/[<AC> 3.2] Clarification on Data Coupling and Control Coupling.

These practices provide complementary information to ED-94C/DO-248C FAQ#67 for satisfying objective A-7 (8) of ED-12C/DO-178C and ED-12B/DO-178B:

a. Data coupling analysis is of a different type and purpose than control coupling analysis. Both analyses are necessary to satisfy this objective.

b. Although they support a verification objective, data coupling and control coupling analyses rely on good practices in the software design phase; for example, through the specification of interfaces (I/O) and of the dependencies between components.

[<AMC> GM3 to AMC 20-115D]/[<AC> 3.3] Error Handling at Design Level.

a. These practices provide complementary information to ED-12C/DO-178C and ED-12B/DO-178B, sections 6.3.2, 6.3.3, and 6.3.4. Section 6.3.4.f. identifies potential sources of errors that require specific activities focused at the source code review level. However, in order to protect against foreseeable unintended software **[**behaviour**]/[**behavior**]**, it is beneficial and recommended to handle these sources of error at the design level.

b. To reduce the possibility of unintended software **[**behaviour**]/[**behavior**]**, consider the following activities:

(1) Identification of foreseeable sources of software errors, which include:

(a) Runtime exceptions or errors like fixed/floating point arithmetic overflow, stack/heap overflow or division by zero.

(b) Data/memory corruption or timing issues like those due to lack of partitioning or to improper interrupt management or cache management.

(c) Features leading to unpredictable program execution like dynamic allocation, out-of-order execution or resource contention.

(2) For each foreseeable source of software error, identification of the associated mitigation.

(3) Specification of protection mechanisms in the software requirements (high level requirements or low level requirements), which in particular include the specification and verification of error-handling mechanisms.

(4) For software levels A and B, recommended mitigations to address dynamic features are runtime protection mechanisms because it is not appropriate to rely solely on probabilistic approaches or static analyses. It may be a good practice to implement such runtime mechanisms for the other software levels.

c. Use of Formal Methods according to ED-216/DO-333 may enhance the detection of runtime errors.

[<AC> 4.0 Related Publications.

a. 14 CFR Applicable Sections. 14 CFR parts 21, 23, 25, 27, 29, 33, and 35.

b. FAA Advisory Circulars (ACs).

(1) AC 20-170, *Integrated Modular Avionics Development, Verification, Integration and Approval using RTCA DO-297 and Technical Standard Order C-153.*

(2) AC 20-171, *Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment*.

(3) AC 20-174, *Development of Civil Aircraft and Systems.*

(4) AC 21-50, *Installation of TSOA Articles and LODA Appliances.*

(5) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes.*

(6) AC 25.1309-1, *System Design and Analysis.*

(7) AC 27-1309*, Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*)*.*

(8) AC 29-1309, *Equipment, Systems, and Installations* (included in AC 29-2, *Certification of Transport Category Rotorcraft*)*.*

(9) AC 33.28-1, *Compliance Criteria for 14 CFR § 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems.*

(10) AC 33.28-2, *Guidance Material for 14 CFR 33.28, Reciprocating Engines, Electrical and Electronic Engine Control Systems*.

(11) AC33.28-3, *Guidance Material For 14 CFR § 33.28, Engine Control Systems.*

(12) AC 35.23-1, Guidance *Material for 14 CFR 35.23, Propeller Control Systems*.

c. Industry Documents.

(1) RTCA DO-178, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 1982 (no longer in print).

(2) RTCA DO-178A, *Software Considerations in Airborne Systems and Equipment Certification*, dated March 1985 (no longer in print).

(3) RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1, 1992.

(4) RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.

(5) RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*, dated December 13, 2011.

(6) RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, dated November 8, 2005.

(7) RTCA DO-330, *Software Tool Qualification Considerations*, dated December 13, 2011.

(8) RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A,* dated December 13, 2011.

(9) RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(10) RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(11) EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print).

(12) EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print).

(13) EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992.

(14) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012.

(15) EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012.

(16) EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012.

(17) EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012.

(18) EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012

(19) EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012.

5.0 Where to Find this AC.

a. You may find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/.

b. If you have suggestions for improvement or changes, you may use the template at the end of this AC.

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to 9-AWA-AVS-AIR500-Coord@faa.gov, or (2) faxing it to the attention of the AIR Directives Management Officer at 202-267-3983.

Subject: _____ Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

☐ In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____

4. Impact assessment (IA)

4.1. How the objectives could be achieved — options

The policy of EASA is to propose harmonised and up-to-date AMC that reflect the state of the art and the best practices for the certification and operation of products. Therefore, there is only one possible option, i.e. Option 1.

Option 0 would not meet the objectives of EASA, which are shared by the FAA.

Table 1: Selected policy options

Option No	*Short title*	**Description**
0		No policy change (no change to the rules; risks remain as outlined in the issue analysis).
1		Amend EASA AMC 20-115C and FAA AC 20-115C. *See Section 2.3 for details.*

4.2. What are the impacts

4.2.1. Safety impact

AMC 20-115C and AC 20-115C already provide for an adequate level of safety. Therefore, the focus of this RMT is not to increase safety.

4.2.2. Environmental impact

None.

4.2.3. Social impact

None.

4.2.4. Economic impact

Option 0: Additional certification workload and potential certification delays remain a burden for applicants due to lack of harmonisation between EASA and the FAA.

Option 1: The harmonisation between the guidance of EASA and that of the FAA will relieve the current issues and allow for a smooth certification process. Harmonised AMC and ACs reflecting the state of the art and the best practices will aid the design, certification and validation processes, thereby reducing the costs.

4.2.5. General aviation and proportionality issues

No issues identified.

4.3. Conclusion

4.3.1. Comparison of options

Only Option 1 would meet both the EASA and the FAA objectives.

Overall, this Option would provide for economic benefits by streamlining the certification process thanks to an increased harmonisation between EASA and the FAA, and without safety, social or environmental consequences.

5. References

5.1. Affected/Related regulations

None.

5.2. Affected EASA decision and FAA Advisory Circular material

— Decision No. 2003/12/RM of the Executive Director of the Agency of 5 November 2003 on general acceptable means of compliance for airworthiness of products, parts and appliances (« AMC-20 »), as amended

— FAA AC 20-115C 'Airborne Software Assurance'

5.3. Other reference documents

— EASA CM No.: EASA CM - SWCEH - 002 'Software Aspects of Certification', Issue 01, Revision 01

— FAA Order 8110.49 'Software Approval Guidelines', Change 1